A TALK ON EXPONENTIAL POLYNOMIALS

AYHAN GÜNAYDIN

Introduction

We are going to prove the following.

Theorem. *(Assuming Schanuel's conjecture) Let $p(X,Y) \in \mathbb{C}[X,Y]$ be irreducible such that both X and Y appear in p. Then there is a generic point on the curve defined by p of the form $(z, \exp(z))$.*

In order to prove this it is enough to show the following. (It is not a trivial reduction; the reader should look at the paper for the details.)

Proposition. *(Assuming Schanuel's conjecture) Let $p(X,Y) \in \mathbb{C}[X,Y]$ be irreducible such that both X and Y appear in p and let K be an algebraically closed subfield of $\mathbb{C}$ of finite transcendence degree. Then there are finitely many $z \in K$ such that $p(z, \exp(z)) = 0$.*

1. Linear equations in fields of finit etranscendence degree

In this section Let K be an algebraically closed subfield of $\mathbb{C}$ of finite transcendence degree containing π and let $\Gamma := \exp(K)$. Here we consider solutions in Γ of

$$(\star) \qquad \lambda_1 x_1 + \cdots + \lambda_k x_k = 1,$$

where $\lambda_1, \ldots, \lambda_k \in K$. We say that a solution $\vec{\gamma} = (\gamma_1, \ldots, \gamma_k)$ in Γ of $(\star)$ is *non-degenerate* if $\sum_{i\in I} \lambda_i \gamma_i \neq 0$ for every nonempty proper subset I of $\{1, \ldots, k\}$.

We begin with some notations that will be useful.

Definition 1.1. Let G be an abelian group, written multiplicatively and for $n > 0$ put $G^{[n]} = \{g^n : g \in G\}$. We say that a subgroup H is *pure* in G if $H \cap G^{[n]} = H^{[n]}$ for all $n > 0$. We say that H is *radical* in G if it is pure in G and it contains all the torsion elements of G.

Given $A \subseteq G$, we set $\langle A \rangle_G$ to be the smallest radical subgroup of G containing A. That is,

$$\langle A \rangle_G = \{g \in G \mid g^n \in [A]_G \text{ for some } n \in \mathbb{N}\}$$

where $[A]_G$ is the subgroup generated by A. When G is clear from the context, we will drop the subscripts and just write $\langle A \rangle$ and $[A]$. For instance throughout this section the ambient group is $\mathbb{C}^\times$ unless explicitly stated otherwise.

Since K is a field of characteristic 0, it is easy to see that Γ is divisible; in particular it is pure in $\mathbb{C}^\times$. Moreover Γ is a radical subgroup of $\mathbb{C}^\times$ since $\sqrt{-1}\pi$ is in K. Therefore, so is $\Gamma \cap K^\times$.

Given $a_1, \dots, a_n$ in $\mathbb{C}$, by $\vec{a}$ we denote the tuple $(a_1, \dots, a_n)$ and $\exp(\vec{a})$ denotes $(\exp(a_1), \dots, \exp(a_n))$.

Note the following straight-forward consequence of Schanuel's Conjecture concerning the rank of $\Gamma \cap K^\times$.

Lemma 1.2. *(Assuming Schanuel's conjecture)*
The rank of $\Gamma \cap K^\times$ is at most d.

On the basis of this lemma, take $\beta_1, \dots, \beta_t \in K$ where $t \le d$ such that $\pi\sqrt{-1}, \beta_1, \dots, \beta_t$ are $\mathbb{Q}$-linearly independent and

$$\Gamma \cap K^\times = \langle \exp(\beta_1), \dots, \exp(\beta_t) \rangle.$$

Recall Lemma 8.2 from [2].

Lemma 1.3. *Let F be a field with a subfield E and subgroups G, H of $F^\times$. Suppose also that H is a radical subgroup of G. Then the following two conditions are equivalent:*

1. *for every $\lambda_1, \dots, \lambda_k \in E$, the equation $(\star)$ has the same non-degenerate solutions in H as in G.*
2. *whenever $g_1, \dots, g_n$ in G are multiplicatively independent over H, they are algebraically independent over the field $E(H)$.*

This allows us to prove the following.

Proposition 1.4. *(Assuming Schanuel's conjecture)*
There exists a radical subgroup Γ^* of Γ of finite rank containing $\Gamma \cap K^\times$ such that for every $\lambda_1, \dots, \lambda_k$ in K, the equation $(\star)$ has the same non-degenerate solutions in Γ^* as in Γ.

Remark. It follows from the proof above that if the rank of $\Gamma \cap K^\times$ is already d, then we can take Γ^* to be $\Gamma \cap K^\times$.

Let $\Gamma^* = \langle \exp(a_1), \dots, \exp(a_s) \rangle$ with $a_1, \dots, a_s \in K$ linearly independent over $\sqrt{-1}\pi$.

From now on, $\mathbb{U}$ denotes the multiplicative group of all roots of unity. Recall the following results.

Lemma 1.5. *(Lemma 6.1 in* [3]*)*
Let $E \subseteq F$ be fields such that $E \cap \mathbb{U} = F \cap \mathbb{U}$ and G be a pure subgroup of $E^\times$. Then for $\lambda_1, \dots, \lambda_n \in E^\times$, the equation $(\star)$ has the same non-degenerate solutions in G as in $\langle G \rangle_{F^\times}$.

Lemma 1.6. *(Proposition 2.2 (ii) in* [10]*)*
Let L be a finitely generated extension of $\mathbb{Q}(\mathbb{U})$. Then the quotient group $L^\times/\mathbb{U}$ is free.

We can now reduce our situation from K to any subfield L that is finitely generated over $\mathbb{Q}(\mathbb{U})$ containing the generators $\exp(\vec{a})$.

Lemma 1.7. *Let L be a finitely generated extension of $\mathbb{Q}(\mathbb{U})$ containing* $\exp(\vec{a})$*. Then there are $c_1, \dots, c_{t'}$ in K linearly independent over $\sqrt{-1}\pi$ such that for every $\lambda_1, \dots, \lambda_k \in L$, all the nondegenerate solutions of $(\star)$ in Γ^* are in $\mathbb{U} \cdot [\exp(\vec{c})]$.*

Proof. ... □

2. Specialisations and reduction to a number field

We first remark the following easy observation, whose proof is in Lemme 4 of [8], which we restate as Lemma 2.3 below (note that there, R is a finitely generated $\mathbb{Q}$-algebra, but the conclusion is stronger).

Lemma 2.1. *Let R be a subring of $\bar{\mathbb{Q}}[S]$, where S is a finite subset of $\mathbb{C}$. Suppose that $b_1, \ldots, b_q$ are elements of R and let q' be the linear dimension over $\bar{\mathbb{Q}}$ of $\vec{b}$. Then there are ring homomorphisms $\phi_1, \ldots, \phi_{q'}$ from R to $\bar{\mathbb{Q}}$ fixing $k := R \cap \bar{\mathbb{Q}}$ such that for every $\alpha_1, \ldots \alpha_q$ in k with $\alpha_1 b_1 + \cdots + \alpha_q b_q \neq 0$ there is some $i \in \{1, \ldots, q'\}$ with $\phi_i(\alpha_1 b_1 + \cdots + \alpha_q b_q) \neq 0$.*

Proof. ... □

In order to reduce our setting to a number field in the next section, we need to carefully choose a specialization to $\bar{\mathbb{Q}}$. This is ensured by the density of closed points in specific subsets of the spectrum of any finitely generated $\mathbb{Q}$-algebra R. Given such R and a polynomial Q over R irreducible in $\mathrm{Frac}(R)[X]$, denote by $\Omega(Q)$ the collection of prime ideals $\mathfrak{p}$ of R such Q mod $\mathfrak{p}$ has the same degree as Q and it is irreducible as a polynomial over $\mathrm{Frac}(R/\mathfrak{p})$. Recall that a *Hilbert set* Ω is a subset of $\mathrm{Spec}(R)$ which contains a finite intersection of non-empty open sets and sets of the form $\Omega(Q)$.

Fact 2.2. Let R be a finitely generated $\mathbb{Q}$-algebra.

- (i) Given a finitely generated subgroup G of $R^\times$, there is a Hilbert set Ω such that the residue map $G \to (R/\mathfrak{p})^\times$ is injective for every $\mathfrak{p}$ in Ω.
- (ii) For any Hilbert set Ω in R, the collection of maximal ideals contained in Ω is dense in $\mathrm{Spec}(R)$.

Combining the above with the proof of Lemma 2.1, one obtains the following result.

Lemma 2.3. *(Lemme 4 in* [8]*)*
Let R be a finitely generated $\mathbb{Q}$-algebra with largest subfield k and G a finitely generated subgroup of $R^\times$. Suppose also that $b_1, \ldots, b_q$ are elements of R that generate a $\bar{\mathbb{Q}}$-linear space of dimension q'. Then there are ring homomorphisms $\phi_1, \ldots, \phi_{q'}$ from R into $\bar{\mathbb{Q}}$ such that each ϕ_i is injective on G and that for every $\alpha_1, \ldots \alpha_q \in k$ with $\alpha_1 b_1 + \cdots + \alpha_q b_q \neq 0$, there is $i \in \{1, \ldots, q'\}$ with

$$\phi_i(\alpha_1 b_1 + \cdots + \alpha_q b_q) \neq 0.$$

In order to bound the degrees of the roots of unity appearing in Lemma 1.7 we will need the following result.

Theorem 2.4. *(Theorem 1 in* [4]*)*
Let F be a number field, $a_0, a_1, \ldots, a_k$ in F and ζ a root of unity of order Q such that $a_0 + \sum_{j=1}^{k} a_j \zeta^{n_j} = 0$ with $\gcd(Q, n_1, \ldots, n_k) = 1$. Let $\delta = [F \cap \mathbb{Q}(\zeta) : \mathbb{Q}]$ and suppose that for any nonempty proper subset I of $\{0, 1, \ldots, k\}$ the sum $\sum_{j \in I} a_j \zeta^{n_j} \neq 0$. Then for each prime p and $n > 0$, if $p^{n+1} | Q$, then $p^n | 2\delta$ and

$$k \geq \dim_F(F + F\zeta^{n_1} + \cdots + F\zeta^{n_k}) \geq 1 + \sum_{p | Q, p^2 \nmid Q} [\frac{p-1}{\gcd(\delta, p-1)} - 1].$$

In particular, the order Q of ζ is bounded by a constant depending on k and δ (and therefore $[F:\mathbb{Q}]$).

The last result of this section concerns work from [7]. Work inside a number field F. For t, r in $\mathbb{N}$ consider polynomials $Q_1,\dots,Q_r$ over F in t many variables as well as a finite set $Z := \{a_{ji} : j=1,\dots,r\,;\ i=1,\dots,t\}$ in $F^\times$. We are interested in describing the set of tuples $\vec{m}$ in $\mathbb{Z}^t$ such that

$$(**) \qquad \sum_{j=1}^{r} Q_j(\vec{m}) \prod_{i=1}^{t} a_{ji}^{m_i} = 0.$$

For such an equation (**), let H be the subgroup of those $\vec{m}$ in $\mathbb{Z}^t$ such that

$$\prod_{i=1}^{t} a_{ji}^{m_i} = \prod_{i=1}^{t} a_{j'i}^{m_i},$$

for every $j, j' \in \{1,\dots,r\}$.

Théorème 6 of [7] describes precisely the solutions of (**), however for our purposes the following simplified version suffices.

Theorem 2.5. *Suppose that H is trivial. Then there are constants δ, η depending only on Z and the field F such that if $\vec{m}$ in $\mathbb{Z}^t$ satisfies (**) and for every nonempty proper $J \subseteq \{1,\dots,r\}$ the sum $\sum\limits_{j\in J} Q_j(\vec{m}) \prod_{i=1}^{t} a_{ji}^{m_i}$ is nonzero, then*

$$||\vec{m}|| \le \delta \log ||\vec{m}|| + \eta,$$

where $||\vec{m}|| := \max_i |m_i|$.

Remark. The independence of the constants δ, η from the coefficients of Q_i follows from the proof of [7]. Therefore, there is some $N \in \mathbb{N}$ such that if $\vec{m}$ satisfies a non-trivial equation (**), then $||\vec{m}|| \le N$.

3. The Main Theorem

We have now all the necessary tools to prove the following result.

Theorem 3.1. *(Assuming Schanuel's conjecture) For an irreducible complex polynomial p in two variables where both variables appear, the entire function $f(z) := p(z, \exp(z))$ has infinitely many algebraically independent zeros.*

Proof. Here we keep the notations from the previous sections. In particular, K is an algebraically closed subfield of $\mathbb{C}$ of finite transcendence degree containing π and the coefficients of p.

Using Hadamard Factorization Theorem (see for instance [6]) and a result proved independently by Henson and Rubel [5] and by van den Dries [1], we have that $f(z) = p(z, \exp(z))$ has infinitely many zeros in $\mathbb{C}$ (for a proof of this, see [9]). Therefore in order to prove our theorem, it suffices to show that $f(z)$ has finitely many zeros in K.

Write

$$p(X,Y) = \sum_{j=0}^{m} p_j(X) Y^j,$$

where $p_j(X) \in K[X]$. Also set $I = \{j \in \{0, \ldots, m\} \mid p_j \neq 0\}$. Since p is irreducible, 0 lies in I. The set $\{z \in \mathbb{C} \mid p_j(z) = 0 \text{ for some } j \in I\}$ is finite. Hence in order to show that there are finitely many solutions in K to $p(z, \exp(z)) = 0$ we need only prove that

$$W = \{z \in K \mid p(z, \exp(z)) = 0 \wedge \bigwedge_{j \in I} p_j(z) \neq 0\}$$

is finite.

Claim. *There are $c_1, \ldots, c_{t'}$ in K linearly independent over $\sqrt{-1}\pi$ such that*

$$W \subseteq \mathbb{Q}\pi\sqrt{-1} + \mathbb{Z}c_1 + \cdots + \mathbb{Z}c_{t'}.$$

Proof. ... ☐

We now apply Theorem 2.4 to get a finer description of W.

Claim. *There is $N \in \mathbb{N}$ such that if $z \in W$ then there are $k, m_1, \ldots, m_{t'}$ in $\mathbb{Z}$ and $0 < n < N$ such that*

$$z = \frac{k2\pi\sqrt{-1}}{n} + \sum_{j=1}^{t'} m_j c_j$$

Proof. ... ☐

Remark. Using this claim we may assume, after modifying f (finitely many times) that its zeroes in K are of the form

$$l2\pi\sqrt{-1} + \sum_{j=1}^{t'} m_j c_j$$

with $l, m_1, \ldots, m_{t'} \in \mathbb{Z}$.

We have reduced the theorem to prove that there are only finitely many $(l, \vec{m})$ such that

$$(***) \quad \sum_{j \in I} p_j(l2\pi\sqrt{-1} + \sum_{j=1}^{t'} m_j c_j)(\vec{d}^{\vec{m}})^j = 0 \text{ and } p_j(l2\pi\sqrt{-1} + \vec{m} \cdot \vec{c}) \neq 0 \text{ for } j \in I.$$

Let R be the $\mathbb{Q}$-algebra generated by the coefficients of p, $\pi\sqrt{-1}$, $\vec{c}$, $\vec{d}$ and their inverses. Let G be the multiplicative subgroup of $R^\times$ generated by $\vec{d}$. Choose $\phi_1, \ldots, \phi_q$ ring homomorphisms from R to $\bar{\mathbb{Q}}$ injective on G as in Lemma 2.3 and let F be the compositum field of all their images.

Let $(l, \vec{m})$ satisfy (***) and choose ν in $\{1, \ldots, q\}$ such that

$$\phi_\nu(p_0(l2\pi\sqrt{-1} + \sum_{j=1}^{t'} m_j c_j)) \neq 0.$$

The map ϕ_ν transforms (***) into

$$\sum_{j \in I} p_{jl}(\vec{m}) \prod_{i=1}^{t'} \phi_\nu(d_i^j)^{m_i} = 0,$$

where $p_{jl}(\vec{X})$ is is a poynomial in $(1+t')$-variables such that

$$p_{jl}(\vec{m}) = \phi_\nu(p_j(l2\pi\sqrt{-1} + \vec{m}\cdot\vec{c})).$$

We may assume that no subsum is zero. Hence applying Theorem 2.5 and the remark after it, there is T in $\mathbb{N}$ independent of l such that $||\vec{m}|| \leq T$. The proof finishes by noting that for each $\vec{m}$, there are finitely many l's satisfying (***). $\square$

References

[1] Lou van den Dries. Exponential rings, exponential polynomials and exponential functions. *Pacific J. Math.*, 113(1):51–66, 1984.

[2] Lou van den Dries and Ayhan Günaydın. The fields of real and complex numbers with a small multiplicative group. *Proc. London Math. Soc. (3)*, 93(1):43–81, 2006.

[3] Lou van den Dries and Ayhan Günaydın. Mann pairs. *Trans. Amer. Math. Soc.*, 362(5):2393–2414, 2010.

[4] Roberto Dvornicich and Umberto Zannier. On sums of roots of unity. *Monatsh. Math.*, 129(2):97–108, 2000.

[5] C. Ward Henson and Lee A. Rubel. Some applications of Nevanlinna theory to mathematical logic: identities of exponential functions. *Trans. Amer. Math. Soc.*, 282(1):1–32, 1984.

[6] Lars Hörmander. *An introduction to complex analysis in several variables*, volume 7 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, third edition, 1990.

[7] Michel Laurent. Equations diophantiennes exponentielles. *Invent. Math.*, 78:299–327, 1984.

[8] Michel Laurent. Équations exponentielles-polynômes et suites récurrentes linéaires. II. *J. Number Theory*, 31(1):24–53, 1989.

[9] David Marker. A remark on Zilber's pseudoexponentiation. *J. Symbolic Logic*, 71(3):791–798, 2006.

[10] Boris Zilber and Martin Bays. Covers of multiplicative groups of algebraically closed fields of arbitrary characteristic. Available at the webpage `www.maths.ox.ac.uk/~zilber`, 2007.